

A TRUE COPY

Jul 21, 2022

s/ Michael Longley

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))(1) a red Apple iPhone with unknown serial number, (2) a gray
Apple iPhone IMEI: 357447882302617, and (3) a white Apple
iPhone IMEI: 359811261098674 (further described in
Attachment A))

Case No.

22-M-499 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure
of the following person or property located in the _____ District of _____


(identify the person or describe the property to be searched and give its location):

See Attachment A. Over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal
Procedure 41.I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 8-3-22 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____Date and time issued: 7-21-22 3:35 pmCity and state: Milwaukee, Wi
Judge's signature

Hon. Stephen C. Dries, Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

The property to be searched includes: : (1) a red Apple iPhone with unknown serial number, (2) a gray Apple iPhone IMEI: 357447882302617, and (3) a white Apple iPhone IMEI: 359811261098674 (collectively the “Devices”) that are currently held as evidence inside the Federal Bureau of Investigation’s Milwaukee Office at 3600 S Lake Drive, St. Francis, WI.

This warrant Authorizes the forensic examination of the Devices for the purposes of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

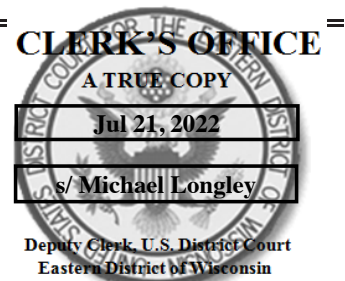
1. All records on the Devices described in Attachment A that relate to violations of Title 21, United States Code, Sections 841 and 846, including but not limited to:
 - a. lists of customers and related identifying information;
 - b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information); and,
 - d. all bank records, checks, credit card bills, account information, and other financial records.
2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Records evidencing the use of the Internet Protocol address to communicate with using the internet including:
 - a. records of Internet Protocol addresses used;
 - b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Case No. **22-M-499 (SCD)**

(1) a red Apple iPhone with unknown serial number, (2) a gray Apple iPhone IMEI: 357447882302617, and (3) a white Apple iPhone IMEI: 359811261098674 (further described in Attachment A)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A. Over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 21, U.S.C. § 841 and 846	Distribution and possession with intent to distribute controlled substances, and conspiracy to distribute and possess with the intent to distribute controlled substances.

The application is based on these facts:

See the attached affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature

TFO Ryan Casey, FBI
 Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ telephone _____ (specify reliable electronic means).

Date: 7-21-22


 Judge's signature

City and state: Milwaukee, Wi

Hon. Stephen C. Dries, Magistrate Judge

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Ryan Casey, a Task Force Officer of the Federal Bureau of Investigation (“FBI”) being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B, based at least in part on personal observations, knowledge and reports written by other law enforcement investigators, which I consider to be truthful and reliable.

2. I have been employed with the Milwaukee Police Department as a full time sworn police officer since 2015. I am currently assigned as a task force officer to the Milwaukee Area Safe Streets Task Force (MASSTF) at the FBI Milwaukee Field Office. In April 2020, I was officially sworn in as a federal task force officer. I have received training in the investigation of drug trafficking. I have participated in search warrants, investigations, and arrests in which controlled substances and drug paraphernalia were seized. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. I have been involved in numerous narcotic and weapon based investigations, during which cellular devices have been seized as evidence relating to narcotic distribution. I know through training and experience, as well through information obtained from other investigators that criminal drug traffickers use cellular devices to store and transmit information to others relating to ongoing criminal drug

trafficking. I know that evidence of drug distribution can be found in the contact lists, photographs, videos, text messages, call logs, internet based applications, and other areas of digital storage within cellular devices that drug traffickers have in their possession.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched includes: (1) a red Apple iPhone with unknown serial number, (2) a gray Apple iPhone IMEI: 357447882302617, and (3) a white Apple iPhone IMEI: 359811261098674 (“the Devices”) that are currently held as evidence inside the Federal Bureau of Investigation’s Milwaukee Office at 3600 S Lake Drive, St. Francis, WI.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. In May 2022, a confidential source (“CS-1”) provided information to agents about Erick A MUNOZ (Hispanic male, DOB: 12/17/1995) and his drug trafficking activities in the Chicago and Wisconsin area. CS-1 stated that MUNOZ contacted CS-1 and offered to sell wholesale quantities of cocaine to CS-1 at his residence in Milwaukee, WI. MUNOZ contacted CS-1 utilizing telephone number (414) 687-5553. Through several consensually recorded phone calls and SMS messages, MUNOZ agreed to retrieve approximately five (5) kilograms of cocaine. The determined price for each kilogram of cocaine was \$28,500 dollars. The five (5) kilograms of cocaine would be exchanged for a total of \$142,500 United States currency.

7. CS-1 has one prior misdemeanor conviction for vandalism. CS-1 is cooperating in hopes of receiving consideration relating to a March 2019 arrest for a attempted purchase of

one kilogram of cocaine. CS-1 has proven reliable and credible, and information provided by CS-1 has led to multiple narcotics seizures and has been corroborated by independent investigative techniques, to include toll records, recorded conversations, and physical surveillance conducted by law enforcement.

8. Over the next several weeks, MUNOZ and CS-1 had multiple conversations via recorded phone calls and SMS messages about the purchase of kilogram quantities of narcotics.

9. Based on the information and the context of the phone calls and text messages between CS-1 and MUNOZ, it was believed that MUNOZ was arranging a narcotics transaction with CS-1 to be conducted at his residence located at 3607 W. Rogers Street, Milwaukee, Wisconsin 53215.

10. Subscriber information on telephone (414) 687-5553 comes back to Erick MUNOZ, 3607 W. Rogers Street, Milwaukee, Wisconsin 53215. A WE energies check confirmed that MUNOZ has been on the utilities account for 3607 W. Rogers Street since 2016. In addition, MUNOZ identified this address in communications with CS-1.

11. Agents accordingly applied for and received a federal search warrant for 3607 W. Rogers Street.

12. On June 21st, 2022, at the direction of handling agents, CS-1 coordinated the sale of five (5) kilograms of cocaine with MUNOZ at his residence located at 3607 W. Rogers Street.

13. Prior to the search warrant being executed, surveillance was conducted around the target residence.

14. At approximately 5:25 pm, law enforcement observed a gray Dodge Ram pickup truck bearing Wisconsin registration plate (SE-6710) pull into the alley behind the residence and briefly stop. Law enforcement observed the Dodge circle the block and again pull into the alley

behind the residence at 3607 W. Rogers Street. The Dodge then parked on the concrete slab behind the residence. The Dodge was occupied by two Hispanic males.

15. Law enforcement observed a Hispanic male, who was wearing a yellow/neon style construction shirt, exit the driver's side door of the Dodge. The unknown Hispanic male then retrieved a dark colored bag from the vehicle and walked up to the southeast door of the target residence and entered.

16. Law enforcement observed an unknown Hispanic male exit the passenger side door of the Dodge and then enter the driver's seat. The Dodge then traveled out of the alley and parked facing northbound near the address of 2078 S. 36th Street. A check of the Wisconsin registration plate for the Dodge showed it lists to a Christopher RUEDA (Hispanic male, DOB: 06/26/1997), with a listed address of 3307 S. 8th Stree, Milwaukee, WI 53215.

17. At the direction of handling agents, CS-1 confirmed that the narcotics were inside the residence and the search warrant was executed.

18. Erick MUNOZ was detained while standing on the stairs leading up to his residence. On his person was a gray Apple iPhone with green rubberized case (one of the Devices).

19. The person that was wearing the yellow/neon style construction shirt and was observed by law enforcement walking up to the residence carrying the bag was detained in the kitchen of 3607 W. Rogers Street. He was identified as Juan D DIAZ (Hispanic male, DOB: 07/31/1989). On his person was a white Apple iPhone with red rubberized case (another of the Devices).

20. During the search of 3607 W. Rogers Street, a purple bag was located inside the kitchen freezer of the residence. Inside the purple bag were six brick shaped objects of a white

substance that was consistent with kilograms of cocaine. Law enforcement confirmed that this was the same purple bag that DIAZ was observed carrying into the residence.

21. During the search of the residence, an active red Apple iPhone was located on top of cabinet in kitchen (the last of the Devices). Also located in the kitchen was a money counter.

22. Five of the suspected kilogram size bricks were vacuum sealed. One of the suspected kilogram bricks was wrapped in a black plastic bag. Presumptive testing was conducted on the white powdery substance utilizing the Nark II Scott Reagent field test. The white substance tested positive for the presence of cocaine.

23. Each kilogram package of cocaine was weighed. The cocaine with packaging was found to weigh approximately 1274.6 grams, 1196.1 grams, 1188.8 grams, 1177.1 grams, 1241.1 grams, and 1272.9 grams.

24. I know that persons who engage in ongoing criminal drug trafficking utilize cellular devices to further their activities. I know that drug traffickers utilize cellular devices to maintain contact with other affiliates and store information relating to drug trafficking. I know that evidence of drug trafficking can be held on the photographs, videos, call logs, text messages, contact lists, and otherwise stored digital information. I know that drug traffickers often record images and/or videos depicting narcotic evidence, maintain contact with others regarding drug trafficking through cellular devices which would be recorded in call logs and text messages, as well as maintain a contact list of affiliates within their cellular devices for personal reference and use. I know that additional evidence of drug trafficking would be stored within other digital stored memory of the cellular devices, and that law enforcement investigators could retrieve the electronically stored evidence if accessible.

25. The Devices are currently in the lawful possession of the Federal Bureau of Investigation. Therefore, while the Federal Bureau of Investigation might already have all necessary authority to examine the devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

26. Based on my training and experience and work with fellow law enforcement, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of the the Federal Bureau of Investigation.

TECHNICAL TERMS

27. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers and devices on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g.,

121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- f. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- g. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

28. Based on my training, experience, knowledge and research, I know that the Devices may have the capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training, experience, knowledge, and research, I have learned that examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

29. Based on my knowledge, training, and experience, I know that electronic devices, like the Devices at issue here, can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct

evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a devices can also indicate who has used or controlled the devices. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property to be searched includes: : (1) a red Apple iPhone with unknown serial number, (2) a gray Apple iPhone IMEI: 357447882302617, and (3) a white Apple iPhone IMEI: 359811261098674 (collectively the “Devices”) that are currently held as evidence inside the Federal Bureau of Investigation’s Milwaukee Office at 3600 S Lake Drive, St. Francis, WI.

This warrant Authorizes the forensic examination of the Devices for the purposes of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 21, United States Code, Sections 841 and 846, including but not limited to:
 - a. lists of customers and related identifying information;
 - b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information); and,
 - d. all bank records, checks, credit card bills, account information, and other financial records.
2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Records evidencing the use of the Internet Protocol address to communicate with using the internet including:
 - a. records of Internet Protocol addresses used;
 - b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review